

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-267462

(43)Date of publication of application : 24.09.1992

(51)Int.Cl. G06F 15/00

G06F 1/00

H04L 9/00

H04L 9/10

H04L 9/12

(21)Application number : 03-028226 (71)Applicant : CANON INC

(22)Date of filing : 22.02.1991 (72)Inventor : FUKUTOME NAOFUMI

(54) SECURITY SYSTEM

(57)Abstract:

PURPOSE: To capable of protecting security even when information such as user ID and a pass-word is revealed by executing the log-in with secret procedure by the insertion of an ID card.

CONSTITUTION: A main memory 6 of a terminal has a log-in procedure storing part 6a to store the log-in proceduce read from an ID card. The terminal, when a log-in request is inputted, reads the log-in procedure written beforehand and information such as a user ID and a pass-word from the ID card inserted by a card reading part 8. The pass-word (for example, group pass-word) different from the information from the ID card is inputted from a keyboard and the log-in is executed by the procedure read from

the ID card. When the writing request to the ID card occurs after the changing of the user ID or the pass-word, a card writing part 9 writes the new information or the procedure into the inserted ID card.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-267462

(43) 公開日 平成4年(1992)9月24日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 G	7323-5L		
1/00	3 7 0 E	7927-5B		
H 0 4 L 9/00				
9/10				
	7117-5K		H 0 4 L 9/00	Z
			審査請求 未請求	請求項の数2(全 4 頁) 最終頁に続く

(21) 出願番号 特願平3-28226

(22) 出願日 平成3年(1991)2月22日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 福留 直文

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 弁理士 大塚 康徳 (外1名)

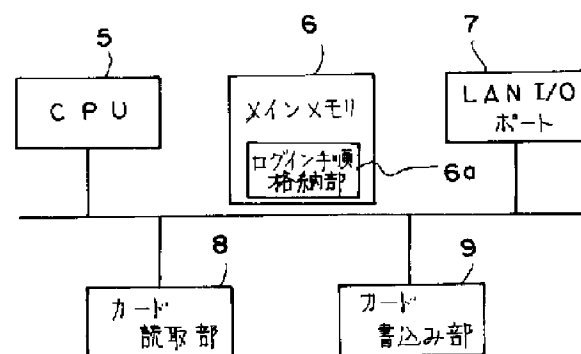
(54) 【発明の名称】 セキュリティ方式

(57) 【要約】

(目的) 本発明は、ユーザIDやパスワード等の情報が知られてもセキュリティを保護可能なセキュリティ方式を提供することを目的とする。

(構成) ログインするための手順と情報とをIDカードから読み取る読取手段と、該手順と情報とに従ってログインするログイン手段とを備え、IDカードの挿入により秘密の手順でログインが実行されることを特徴とする。更に、ログインするための手順を更新する手段と、該更新された手順をIDカードに書き込む手段とを備えることを特徴とする。

第3図



【特許請求の範囲】

【請求項1】 ログインするための手順と情報とをIDカードから読み取る読取手段と、該手順と情報とに従ってログインするログイン手段とを備え、IDカードの挿入により秘密の手順でログインが実行されることを特徴とするセキュリティ方式。

【請求項2】 ログインするための手順を更新する手段と、該更新された手順をIDカードに書き込む手段とを更に備えることを特徴とする請求項1に記載のセキュリティ方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はネットワークにおけるセキュリティ方式、特にIDカードを使用する場合のセキュリティ方式に関するものである。

【0002】

【従来の技術】 従来、IDカードには個人を識別するための情報が入力されており、ビルの出入口でのチェック等に用いられている。一方、ネットワークシステムにおいては、通常ホストコンピュータへのログインは端末からのキー入力で行うようになっていた。

【0003】

【発明が解決しようとしている課題】 しかしながら、上記従来例では、ユーザIDやパスワード等の情報を部外者に知られやすいという欠点があった。

【0004】 本発明は、前記従来例の欠点を除去し、ユーザIDやパスワード等の情報が知られてもセキュリティを保護可能なセキュリティ方式を提供する。

【0005】

【課題を解決するための手段】 この課題を解決するために、本発明のセキュリティ方式は、ログインするための手順と情報とをIDカードから読み取る読取手段と、該手順と情報とに従ってログインするログイン手段とを備え、IDカードの挿入により秘密の手順でログインが実行される。更に、ログインするための手順を更新する手段と、該更新された手順をIDカードに書き込む手段とを備える。

【0006】 かかる構成により、部外者にユーザIDやパスワード等の情報を容易には知られないようにしたものである。また、部外者が不正にIDカードを取得した場合でも、容易にはネットワークに侵入されないようにしたものである。

【0007】

【実施例】 図1は本発明のセキュリティ方式を実施するネットワークシステムの構成を示すブロック図である。1はユーザに種々のサービスを提供するホストコンピュータ、2、3はサービスを受けるための端末、4はホストコンピュータ及び端末2、3を接続するLANである。

【0008】 図2はホストコンピュータ1のハードウエ

ア構成を示すブロック図である。11は本発明のセキュリティ方式を含む種々のサービスをプログラムとして実行するCPU、12は現在の各ユーザのパスワード及びグループパスワードを格納するパスワードテーブル、13はプログラムをロードするためのメインメモリであると共に、ユーザのIDカードに書き込むための最新のログイン手順を記憶する最新ログイン手順記憶部13aを有する。14はLANとの間のデータの入出力を制御するためのLAN I/Oポートである。

10 【0009】 図3は端末2、3のハードウェア構成を示すブロック図である。5は図5に示すようなソフトウェアをプログラムとして実行するCPU、6はプログラムをロードするためのメインメモリであると共に、ユーザのIDカードから読み込んだログイン手順を格納するログイン手順格納部6aを有している。7はLANとの間のデータの入出力を制御するためのLAN I/Oポート、8はIDカードからログインの手順と情報とを読み取るためのカード読取り部、9は新しい手順と情報とをIDカードに書き込むためのカード書込み部、10はパスワード等を入力するためのキーボードである。

【0010】 図4はホストコンピュータ1上で動作するソフトウェアのモジュール構成図である。図5は端末2、3上で動作するソフトウェアのモジュール構成図である。ここで、TCP(Transmission Control Protocol)、IP(Internet Protocol)、LLC(Logical Link Control)、DLC(DataLink Control)であり、以下に簡単に説明する。

【0011】 TCP/IPは、アメリカ国防省がコンピュータネットワークを信頼性の高いものにするために作ったプロトコルである。TCPは、ネットワークに存在する2つのノード間をエンド・ツー・エンドで接続し、アプリケーション・プログラムに高品質で信頼性の高い通信機能を提供するための手順であり、順序制御、フロー制御などの機能を持っている。OSIでは第4層のトランスポート層および第5層のセッション層に相当する。IPは、複数のネットワーク間で途中のネットワークの遅延を吸収し、2つのノード間に透過な経路を作るための手順であり、グローバルなアドレスの割り付け、ルーティング(経路選択)などの機能を持っている。OSIでは第3層のネットワーク層に相当する。

【0012】 LLC/DLCは、IEEE802委員会で制定されたLANのデータリンク層のためのプロトコルである。LLCは、通信媒体の際を吸収し均一な隣接ノード間でのデータ転送機能を提供するための手順である。OSIでは第2層のデータリンク層の上位副層に相当する。DLCは、通信媒体ごとに異なるデータ転送機能を提供するための手順であり、例えばイーサネットの場合はIEEE802.3のように、IEEEでその手順の内容が規定されている。MAC(Media Access Control)と呼ばれることもあり、OSIでは第2層の下位副

層に相当する。なお、OSIとの関係を示すと、次のようになる。OSI L
AN

第7層 アプリケーション
第6層 プレゼンテーション
第5層 セッション TCP
第4層 トランスポート TCP
第3層 ネットワーク IP
第2層 データリンク LLC/DLC
第1層 フィジカル

図6、図7は端末上のソフトウェアの動作を示すフローチャートである。以下、このフローチャートに従って、本実施例の動作手順を説明する。

【0013】まず、端末のシステム立上げ後は、ステップS1でユーザからの要求待ちの状態となつている。ここで、ユーザからログイン要求が入力されるとステップS3からS6に進んで、カード読取り部8で挿入されたIDカードから予め書込まれていたログイン手順とユーザIDやパスワード等の情報とを読み取り、ステップS7ではIDカードからの情報とは別のパスワード（例えばグループパスワード）をキーボードか10から入力させ、ステップS8で読みとられた手順でログインを実行する。

【0014】ログイン手順が正常に終了、つまりログインできた場合には、ステップS9からS1に戻り、再び要求待ちの状態に戻る。また、手順の途中でパスワード入力ミス等正常に終了できなかった場合には、ステップS10でエラー処理を行つた後にステップS1に戻り、要求待ちの状態に戻る。

【0015】また、ユーザIDあるいはパスワードの変更等を行つた後に、IDカードへの書き込み要求が発生した場合は、ステップS2からS5に進んでカード書き込み部9により挿入されているIDカードに新しい情報あるいは手順を書込んだ後にステップS1に戻り、要求待ちの状態に戻る。

【0016】ログイン及びカード書き込み以外の要求が発

生した場合には、ステップS4でその要求に対応した処理を行つた後に、ステップS1に戻り要求待ちの状態に戻る。

【0017】

【発明の効果】本発明により、ユーザIDやパスワード等の情報が知られてもセキュリティを保護可能なセキュリティ方式を提供できる。

【0018】すなわち、ログインする手順と必要な情報をIDカードに入力する手段と、IDカードからその手順と情報を読み取つて実行してホストにログインする手段を端末に設けたことにより、部外者にユーザIDやパスワード等の情報を知られにくくするとともに、ログイン時の操作を簡単にする効果がある。また、ログイン時に別にパスワードを入力する手段を端末に設けたことにより、部外者が不正にIDカードを取得した場合でも容易にはネットワークに侵入できないという効果がある。

【図面の簡単な説明】

【図1】本発明のセキュリティ方式を実施するネットワークシステムの構成を示すブロック図である。

【図2】ホストコンピュータのハードウェア構成を示すブロック図である。

【図3】端末のハードウェア構成を示すブロック図である。

【図4】ホストコンピュータ上で動作するソフトウェアのモジュール構成図である。

【図5】端末上で動作するソフトウェアのモジュール構成図である。

【図6】、

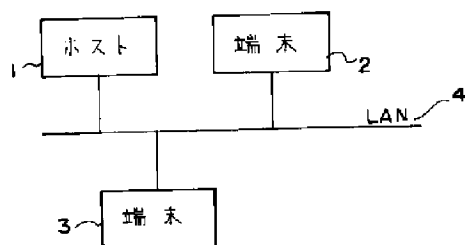
【図7】端末上のソフトウェアの動作手順を示すフローチャートである。

【符号の説明】

1…ホストコンピュータ、2、3…端末、4…LAN、5…CPU、6…メインメモリ、6a…ログイン手順格納部、7…LAN I/Oポート、8…カード読取り部、9…カード書き込み部、10…キーボード、11…CPU、12…パスワードテーブル、13…メインメモリ、13a…最新ログイン手順記憶部、14…LAN I/Oポート

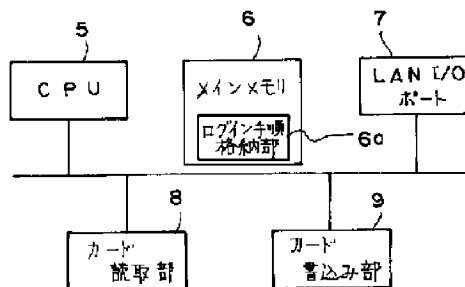
【図1】

第1図



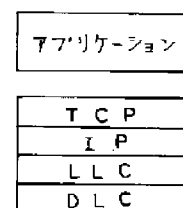
【図3】

第3図

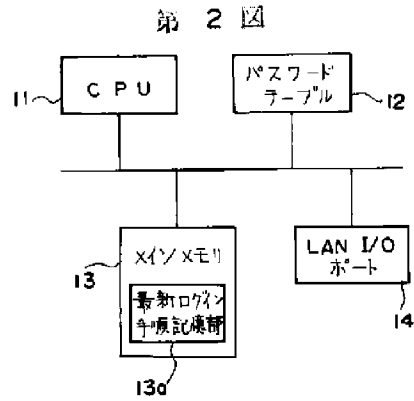


【図5】

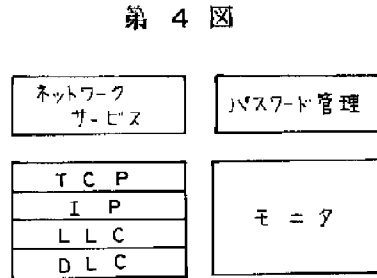
第5図



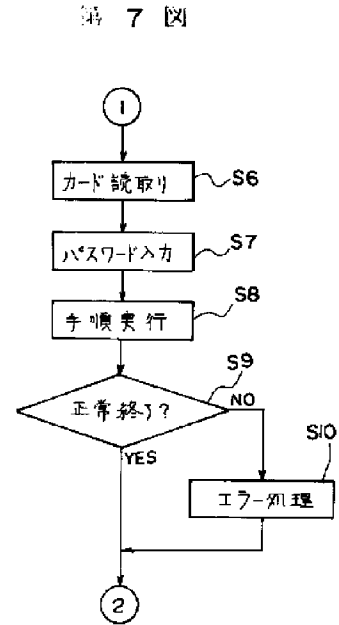
【図2】



【図4】

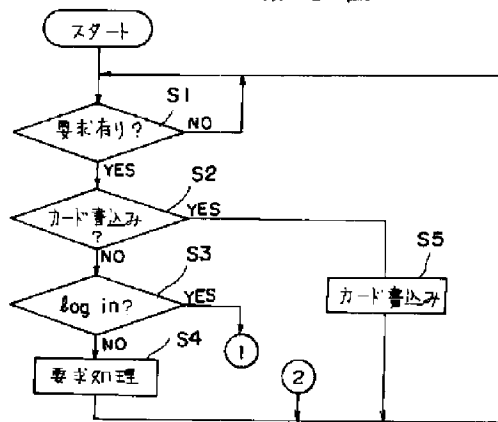


【図7】



【図6】

第 6 図



フロントページの続き

(51) Int. Cl.⁵

H04L 9/12

識別記号

庁内整理番号

F I

技術表示箇所